ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	April 3, 2006	Phone Number	Fax Number
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P393_01.162.01 **App. No: 10/061,415**

Total Number of Pages Being Transmitted, Including Cover Sheet: 38

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

April 3, 2006

Practitioner's Docket No. NAI1P393/01.162.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Davide Libenzi et al.

Application No.: 10/061,415 Group No.: 2131
Filed: February 1, 2002 Examiner: Henning, M.
For: SYSTEM AND METHOD FOR PROVIDING PASSIVE SCREENING OF TRANSIENT MESSAGES IN A DISTRIBUTED COMPUTING ENVIRONMENT

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on February 3, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. " 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is *mandatory;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION
✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 -8300.

Date: 4/3/06

Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P393).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P393).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Practitioner's Docket No. NAI1P393/01.162.01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Davide Libenzi et al.

Application No.: 10/061,415 Group No.: 2131
Filed: February 1, 2002 Examiner: Henning, M.
For: SYSTEM AND METHOD FOR PROVIDING PASSIVE SCREENING OF TRANSIENT MESSAGES IN A DISTRIBUTED COMPUTING ENVIRONMENT

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on February 3, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. " 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is *mandatory;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 -8300.

Date: 4/3/06

Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

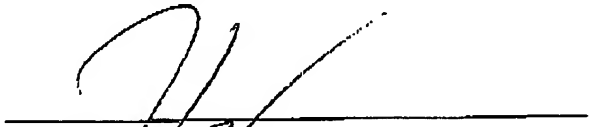
6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P393).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P393).



Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
Libenzi et al.	)	Group Art Unit: 2131
Application No. 10/061,415	)	Examiner: Henning, Matthe
Filed: February 1, 2002	)	Date: April 3, 2006
For: SYSTEM AND METHOD FOR PROVIDING PASSIVE SCREENING OF TRANSIENT MESSAGES IN A DISTRIBUTED COMPUTER ENVIRONMENT)	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 3, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI ISSUES
VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-10, 13-25, 28-38, 40-47 and 49-55

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-10, 13-25, 28-38, 40-47 and 49-55
3. Claims allowed: None
4. Claims rejected: 1-10, 13-25, 28-38, 40-47 and 49-55
5. Claims cancelled: 11-12, 26-27, 39, and 48

C. CLAIMS ON APPEAL

The claims on appeal are: 1-10, 13-25, 28-38, 40-47 and 49-55

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1 and 16, as shown in Figure 2, a system and method are provided for passive screening of transient messages in a distributed computing environment, including a network interface that passively monitors a transient packet stream at a network boundary in which incoming datagrams structured in compliance with a network protocol layer are received (e.g. item 34 of Figure 2). Also included is a packet receiver that reassembles one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer (e.g. item 33 of Figure 2), and an antivirus scanner that scans contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents (e.g. item 32 of Figure 2). In use, a protocol-specific module processes each reassembled datagram based on the transport protocol layer employed by the reassembled datagram (e.g. items 35-58 of Figure 2). See page 7, line 14-page 8, line 5, for example.

With respect to a summary of Claims 32 and 41, as shown in Figure 2, a system and method are provided for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, including a network interface that receives copies of datagrams transiting a boundary of a network domain into an incoming packet queue, where each datagram is copied from a packet stream (e.g. item 34 of Figure 2). Also included is a packet receiver reassembling one or more such datagrams from the incoming packet queue into network protocol packets (e.g. item 33 of Figure 2), each staged in a reassembled packet queue, and an antivirus scanner that scans each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (e.g. item 32 of Figure 2). In use, an event correlator evaluates events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain (e.g. item 31 of Figure 2), and each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram (e.g. items 35-38 of Figure 2). See page 7, line 14-page 8, line 5, for example.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Issue # 2: The Examiner has rejected Claims 32-38, 40-47 and 49-54 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue # 3: The Examiner has rejected Claims 1-10, 13-14, 16-25, 28-29, 31 and 55 under 35 U.S.C. 102(e) as being anticipated by Maher III et al., U.S. Patent No. 6,381,242.

Issue # 4: The Examiner has rejected Claims 32-35, 38, 41-44, 47 and 50-52 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, as evidenced by Stevens (TCP/IP Illustrated Vol. 1).

Issue # 5: The Examiner has rejected Claims 15, 30, 40 and 49 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Hailpern et al., U.S. Patent No. 6,275,937.

Issue # 6: The Examiner has rejected Claims 36-37 and 45-46 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Bates et al., U.S. Patent No. 6,785,732.

Issue # 7: The Examiner has rejected Claims 53-54 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Epstein et al., U.S. Patent No. 6,684,329.

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Specifically, the Examiner has argued that Claims 32 and 41 recite that "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram," but that there is no support for such limitation in the specification. The Examiner has also argued that Claims 53-54 recite "a plurality of protocol-specific scanning submodules, each protocol specific scanning sub-module designated for scanning network protocol packets of a particular protocol," but that there is also no support for such limitation in the specification.

Appellant respectfully points out page 7, line 29-page 8, line 5 which clearly supports such claim language:

> "The antivirus scanner 32 includes a plurality of protocol-specific scanning submodules 35-38, including submodules for the Hypertext Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), and Network News Transport Protocol (NNTP), although other upper layer network protocols could also be implemented, as would be recognized by one skilled in the art.
>
> Through each protocol-specific submodule 35-38, the antivirus scanner 32 retrieves each re-assembled packet from the appropriate protocol-specific queue 41 for scanning using standard antivirus techniques, as are known in the art."

Issue # 2:

The Examiner has rejected Claims 32-38, 40-47 and 49-54 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

The Examiner has stated that Claims 32 and 41 recite that "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram," but that "there is no support for a plurality of separate modules which each process each datagram.

First, appellant respectfully points out that, as claimed, "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram" (emphasis added), and not necessarily that each separate module processes each datagram as the Examiner seems to contend. Second, appellant respectfully asserts that page 7, line 29-page 8, line 5 in the specification clearly supports such claim language.

Since the Examiner rejected Claims 33-38, 40, 42-47 and 49-54 by virtue of their dependency on Claims 32 and 41, appellant respectfully asserts that such rejection is avoided in view of the arguments made above.

The Examiner has stated that Claims 53-54 recite "a plurality of protocol-specific scanning submodules, each protocol specific scanning sub-module designated for scanning network protocol packets of a particular protocol," but that "there is not support in the specification that the scanning sub-modules actually scan the packets."

Appellant respectfully points out the following language from the specification which clearly supports such claim language:

> "**The antivirus scanner 32 includes a plurality of protocol-specific scanning submodules 35-38**, including submodules for the Hypertext Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), and Network News Transport Protocol (NNTP), although other upper layer network protocols could also be implemented, as would be recognized by one skilled in the art.

Through each protocol-specific submodule 35-38, the antivirus scanner 32 retrieves each re-assembled packet from the appropriate protocol-specific queue 41 for **scanning** using standard antivirus techniques, as are known in the art." (Page 7, line 29-Page 8, line 5-emphasis added).

Issue # 3:

The Examiner has rejected Claims 1-10, 13-14, 16-25, 28-29, 31 and 55 under 35 U.S.C. 102(e) as being anticipated by Maher III et al., U.S. Patent No. 6,381,242.

Group #1: Claims 1-2, 5, 7-10, 13-14, 16-17, 20, 22-25, 31, 28-29

With respect to independent Claims 1 and 16, the Examiner has relied on the following excerpts from Maher to make a prior art showing of appellant's claimed "network interface passively monitoring a transient packet stream at a network boundary" (see the same or similar, but not identical language in each of the foregoing claims).

> "Network apparatus 100 accepts data from the line by means of input physical interface 102. Input physical interface 102 can consist of a plurality of ports, and can accept any number of network speeds and protocols, including such high speeds as OC-3, OC-12, OC-48, and protocols including 10/100 Ethernet, gigabit Ethernet, and SONET. **Input physical interface 102 takes the data from the physical ports, frames the data, and then formats the data...**" (Col. 5, lines 46-54-emphasis added)
>
> "QoS processor 116 is operable to perform the **traffic flow management** for the stream of data packets processed by network apparatus 100." (Col. 7, lines 13-15-emphasis added)

Appellant respectfully asserts that such excerpts do not meet appellant's specific claim language. In particular, Maher teaches taking data from physical ports, framing the data, and formatting the data along with a processor that performs traffic flow management (see emphasized excerpts above). Clearly, acting on data, as described in Maher, does not meet appellant's claimed "passively monitoring a transient packet stream at a network boundary" (emphasis added).

In the latest Office Action dated 11/9/2005, the Examiner has responded to appellant's arguments by stating that the claim requires only that the "network interface" be passive. The

Examiner has further argued that Col.5, lines 42-57 in Maher discloses that the fast path data bus receives the framed and formatted data from the physical interface. First, appellant respectfully asserts that the fast path data bus 126 in Maher is connected to a physical network interface 102, such that the fast path data bus 126 feeds data received at the input physical interface 102 to a scanner. Thus, the fast path data bus 126 in Maher is an intermediary between the physical network interface 102 and the scanner, but is not itself a network interface in the manner claimed by appellant (see Figure 2 in Maher). Second, the fast path data bus 126 in Maher does **not** "passively monitor...a transient packet stream at a network boundary," as claimed by appellant since the fast path data bus "feeds the data to traffic flow scanning processor" (emphasis added).

Still with respect to independent Claims 1 and 16, the Examiner has relied on the following excerpt from Maher to make a prior art showing of appellant's claimed "packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer" (see the same or similar, but not identical, language in each of the foregoing claims).

> "The data is first sent to header preprocessor 104, which is operable to perform several operations using information contained in the data packet headers. Header preprocessor 104 stores the received data packets in packet storage memory 106 and scans the header information. The header information is scanned to identify the type, or protocol, of the data packet, which is used to determine routing information and to decode the IP header starting byte. As will be discussed below, network apparatus 100, in order to function properly, needs to reorder out of order data packets and reassemble data packet fragments." (Col. 5, line 60-Col. 6, line 4)

Appellant respectfully asserts that such excerpt generally teaches that the network apparatus "need[s] to reorder out of order data packets and reassemble data packet fragments" (see emphasized excerpt). However, such excerpt does not teach that the "one or more datagrams [are reassembled] into a segment structured in compliance with a transport layer protocol," as specifically claimed by appellant (emphasis added).

In the latest Office Action dated 11/9/2005, it seems the Examiner has failed to respond to appellant's specific arguments. The closest argument the Examiner has made with respect to such claim language is the Examiner's argument (iv) that Maher discloses assembling ATM cells (data link layer datagrams) into complete data packets, which constitute network protocol

packets" (Col. 6, lines 4-7). However, appellant notes that such argument fails to address appellant's claimed "segment structured in compliance with a transport layer protocol" (emphasis added). Furthermore, appellant respectfully asserts that such excerpt only teaches "reassembl[ing] data packet fragments...into complete data packets," but not specifically that such packet are reassembled "into a segment structured in compliance with a transport protocol layer," as claimed by appellant (emphasis added).

In addition, with respect to independent Claims 1 and 16, the Examiner has relied on Col. 7, lines 18-30 in Maher to make a prior art showing of appellant's claimed "protocol-specific module processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram." Appellant respectfully asserts that such excerpt teaches "assign[ing] the data packet to one of [the Qos processor's] internal quality of service queues 132 based on the conclusion [of the header preprocessor and/or the content processor]." However, the sending of the packets to the queues is only performed by the QoS processor 116. Appellant respectfully points out that Maher only utilizes a single QoS processor (see item 116 in Figure 2), but does not teach that such processor is protocol-specific, as claimed by appellant.

Further, the only protocol mentioned in the context of the Maher excerpt relied on by the Examiner relates to a protocol of a data packet (see Col. 5, lines 65-66). Clearly, simply assigning a packet to a queue and/or, in a separate context, determining a protocol of a data packet, as in Maher, does meet appellant's claimed specific claim language, namely "processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram" (emphasis added).

In the latest Office Action dated 11/9/2005, the Examiner has responded to appellant's arguments by stating that "Maher disclosed queuing the packets based on the application type of the packet (i.e. email, VoIP, etc.) in Col. 7, Paragraph 3." The Examiner has argued that the "application type is the application layer data which could not have been accessed until transport layer processing had been performed" and therefore "it was inherent that Maher performed transport layer processing in order to access the application layer data."

Appellant respectfully asserts that Maher teaches a "QoS processor 116 [that] takes the conclusion of either or both of header preprocessor 104 and content processor 110 and assigns the data packet to one of its internal quality of service queues 132 based on the conclusion." However, appellant notes that the conclusion of the header preprocessor relates to routing instructions associated with a data packet (see Col. 6, lines 39-46), and that the conclusion of the content processor relates to scanning the contents of a data packet against a database of signatures (Col. 6, lines 59-63). Thus, in Maher the data packets are assigned to a quality of service queue based on routing information associated with the packet and a scanning performed on the packet, and not "based on the application type of the packet," as the Examiner contends.

Furthermore, appellant respectfully asserts that an application type associated with a packet is not associated with a transport protocol layer of the packet, as the Examiner contends, since a transport protocol layer only relates to a format for transmitting data over a network and not an application type of the data. Thus, it would **not** have been inherent that Maher perform transport layer processing in order for the QoS to assign data packets to queues based on the conclusion of the header preprocessor and the content processor. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Maher reference, since Maher fails to at least suggest all of appellant's claim limitations, as noted above.

Group #2: Claims 3 and 18

The Examiner has relied on Col. 5, line 65-Col. 6, line 1 to make a prior art showing of appellant's claimed "network protocol-specific decoder [that] decod[es] the reassembled segment prior to scanning." Appellant respectfully asserts that such excerpt merely teaches decoding the IP header starting byte, and NOT the reassembled segment, as specifically claimed by appellant. In addition, the IP header starting byte is decoded before being sent to the content processor, which reassembles the data packet (see Col. 6, lines 8-12), and thus Maher does NOT teach decoding the already reassembled segment prior to scanning, in the manner claimed by appellant.

In the latest Office Action dated 11/9/2005, the Examiner has responded to appellant's arguments by stating that Col. 9, lines 29-32 in Maher discloses decoding the data to be scanned by removing the white spaces from the data. The Examiner has also argued that "it was inherent that the packets were decoded in order to access the payload for scanning."

Appellant respectfully asserts that the disclosure relied on by the Examiner only teaches a string preprocessor 360 in a content scanning engine 306 that "is operable to simplify the context by performing operations such as compressing whitespace." However, simply nowhere does Maher even suggest that such string preprocessor or even content processor is a "network protocol-specific decoder," as claimed by appellant (emphasis added). In fact, Maher discloses that the "content processor 110 is operable to scan the contents of data packets forwarded from header preprocessor 104" (Col. 8, lines 35-37), where the header preprocessor is fed the data received from a high-speed network line (Col. 5, lines 42-60). Clearly, Maher teaches that all data packets are fed to the header preprocessor and that "[a]fter [the] data packets have been processed by header preprocessor 104 the data packets...are sent on fast-data path 126 to the...content processor" (Col. 6, lines 8-12). Thus, since the string preprocessor and the content processor accept all data packets, they cannot be network protocol-specific decoders, in the manner claimed by appellant.

In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Again, appellant respectfully asserts that Maher fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #3: Claims 4 and 19

The Examiner has relied on Col. 7, lines 30-33 in Maher to make a prior art showing of appellant's claimed technique "wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware." Appellant respectfully asserts that such excerpt teaches selectively discarding "[i]nformation in queues that do not have the available bandwidth to transmit all the data currently residing in the queue." Clearly, discarding information based on an available bandwidth, as in Maher, does not meet any sort of "terminat[ing] the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware," as claimed by appellant (emphasis added).

In the latest Office Action dated 11/9/2005, the Examiner has relied on Col. 9, line 58-Col. 10, lines 30 in Maher in stating that "Maher disclosed that once the scanning engine had determined that the[re] was not match, the scanning was complete and not further data was required for that flow." Appellant respectfully asserts that such excerpt only discloses that the "scanning is complete and there is or isn't a match," and not that depending on whether there is a match, the scanning terminates, as the Examiner has argued.

Again, appellant respectfully asserts that Maher fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #4: Claims 6 and 21

The Examiner has relied on Col. 10, lines 42-46 in Maher to make a prior art showing of appellant's claimed technique "wherein the action comprises at least one of logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram; and acquiescing to the infection." Appellant respectfully asserts that such excerpt in Maher only teaches that "the content processor can act to alter the bits of [an] infected attachment essentially

rendering the email harmless" (emphasis added). Clearly, altering the bits of an infected attachment does not meet appellant's specific claim language, namely "logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram; and acquiescing to the infection."

In the latest Office Action dated 11/9/2005, the Examiner has argued that Col. 10, lines 42-46 meets appellant's claimed "spoofing." Appellant respectfully asserts that such excerpt only teaches "alter[ing] the bits of [an] infected attachment [for] essentially rendering the email harmless." Clearly, only altering bits of an email attachment to render the email harmless does not meet any sort of "spoofing," let alone spoofing "a valid datagram in place of the infected datagram," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that Maher fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #5: Claim 55

The Examiner has relied on Col. 6, lines 4-7 and Col. 7, paragraph 3 in Maher to make a prior art showing of appellant's claimed technique "wherein incoming datagrams include IP datagrams that are reassembled into TCP segments." The Examiner has specifically argued that "it was inherent that the PDUs of the email data was processed to TCP segments in order to get the payload of the data for scanning." Appellant respectfully disagrees. Simply because the data may be an email does not inherently mean that it must be processed to TCP segments since e-mail may employ various protocols, including IMAP, POP3, SMTP and HTTP. Thus, appellant's specific claim language would not have been inherent in Maher simply because Maher discloses packets that may be associated with emails.

In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Again, appellant respectfully asserts that Maher fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Issue # 4:

The Examiner has rejected Claims 32-35, 38, 41-44, 47 and 50-52 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, as evidenced by Stevens (TCP/IP Illustrated Vol. 1).

Group #1: Claims 32-35, 38, 41-44, 47 and 50-51

With respect to independent Claims 32 and 41, the Examiner has relied on the same rejections with respect to independent Claim 1 in Issue #1, Group #1 above to meet appellant's claim language. However, appellant notes that the excerpts in Maher relied by the Examiner fail to disclose any sort of "receiving copies of datagrams," let alone "into an incoming packet queue," as claimed by appellant (emphasis added).

In the latest Office Action dated 11/9/2005, the Examiner has responded to appellant's arguments by stating that "Maher disclosed receiving data that was taken from the physical ports, framed, and formatted in Col. 5, lines 42-57." The Examiner has concluded that such constitutes "copied datagrams" because the data was copied from the data present at the physical ports.

Appellant respectfully asserts that such excerpt from Maher expressly discloses that the "[i]nput physical interface 102 takes the data from the physical ports, frames the data, and then formats the data for placement on fast-path data bus 126." Thus, in Maher the actual data from the physical ports is received, and not copies of the data, in the manner claimed by appellant.

Still with respect to independent Claims 32 and 41, the Examiner has relied on Col. 5, line 60-Col. 6, line 4 in Maher to make a prior art showing of appellant's claimed "packet receiver reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue" (see the same or similar, but not identical, language in each of the foregoing claims). However, appellant notes that such excerpt does not

specifically teach "reassembling one or more such datagrams...into network protocol packets," as claimed by appellant (emphasis added). In addition, nowhere in the Maher reference is there any disclosure of staging each reassembled datagram "in a reassembled packet queue," in the manner specifically claimed by appellant.

In the latest Office Action dated 11/9/2005, the Examiner has argued that Maher discloses assembling ATM cells (data link layer datagrams) into complete data packets, which constitute network protocol packets" (Col. 6, lines 4-7). Appellant notes, however, that the Examiner has failed to address appellant's argument that nowhere in the Maher reference is there any disclosure of staging each reassembled datagram "in a reassembled packet queue," in the manner specifically claimed by appellant (emphasis added). Appellant respectfully asserts that in Maher "[a]fter the data packets have been processed by the header preprocessor [such that have been reassembled] the data packets...are stored in packet storage memory" (Col. 6, lines 8-14). Clearly, a packet storage memory does not meet appellant's specifically claimed "reassembled packet queue" (emphasis added).

In addition, with respect to independent Claims 32 and 41, the Examiner has relied on Col. 7, lines 18-30 in Maher to make a prior art showing of appellant's claimed technique "wherein each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram." Appellant respectfully asserts that such excerpt teaches "assign[ing] the data packet to one of [the Qos processor's] internal quality of service queues 132 based on the conclusion [of the header preprocessor and/or the content processor]." Appellant respectfully points out that Maher only utilizes a single QoS processor that assigns the packets to queues (see item 116 in Figure 2), and therefore *teaches away* from "a plurality of protocol-specific modules [that] process each reassembled datagram," in the context claimed by appellant (emphasis added).

Further, the only protocol mentioned in the context of the Maher excerpt relied on by the Examiner relates to a protocol of a data packet (see Col. 5, lines 65-66). Clearly, simply assigning a packet to a queue and/or, in a separate context, determining a protocol of a data packet, as in Maher, does meet appellant's specific claim language, namely "processing each

reassembled datagram based on the transport protocol layer employed by the reassembled datagram" (emphasis added).

In the latest Office Action dated 11/9/2005, the Examiner has responded to appellant's arguments by stating that "Maher disclosed queuing the packets based on the application type of the packet (i.e. email, VoIP, etc.) in Col. 7, Paragraph 3." The Examiner has argued that the "application type is the application layer data which could not have been accessed until transport layer processing had been performed" and therefore "it was inherent that Maher performed transport layer processing in order to access the application layer data."

Appellant respectfully asserts that Maher teaches a "QoS processor 116 [that] takes the conclusion of either or both of header preprocessor 104 and content processor 110 and assigns the data packet to one of its internal quality of service queues 132 based on the conclusion." However, appellant notes that the conclusion of the header preprocessor relates to routing instructions associated with a data packet (see Col. 6, lines 39-46), and that the conclusion of the content processor relates to scanning the contents of a data packet against a database of signatures (Col. 6, lines 59-63). Thus, in Maher, the data packets are assigned to a quality of service queue based on routing information associated with the packet and a scanning performed on the packet, and not "based on the application type of the packet," as the Examiner contends.

Furthermore, appellant respectfully asserts that an application type associated with a packet is not associated with a transport protocol layer of the packet, as the Examiner contends, since a transport protocol layer only relates to a format for transmitting data over a network and not an application type of the data. Thus, it would **not** have been inherent that Maher perform transport layer processing in order for the QoS to assign data packets to queues based on the conclusion of the header preprocessor and the content processor. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 52

The Examiner has relied on Col. 3, last paragraph, in Maher to make a prior art showing of appellant's claimed technique "wherein only datagrams compliant with IP protocol are reassembled." Appellant respectfully asserts that such excerpt only generally discloses an IP network. Simply because the network in Maher may include an IP network does not suggest that "only datagrams compliant with IP protocol are reassembled," as claimed by appellant (emphasis added).

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 5:

The Examiner has rejected Claims 15, 30, 40 and 49 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Hailpern et al., U.S. Patent No. 6,275,937.

Group #1: Claims 15, 30, 40 and 49

Appellant respectfully asserts that the subject matter of such claims is deemed novel in view of the arguments made hereinabove.

Issue # 6:

The Examiner has rejected Claims 36-37 and 45-46 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Bates et al., U.S. Patent No. 6,785,732.

Group #1: Claims 36-37 and 45-46

Appellant respectfully asserts that the subject matter of such claims is deemed novel in view of the arguments made hereinabove.

Issue # 7:

The Examiner has rejected Claims 53-54 under 35 U.S.C. 103(a) as being unpatentable over Maher III et al., U.S. Patent No. 6,381,242, in view of Epstein et al., U.S. Patent No. 6,684,329.

Group #1: Claims 53-54

Appellant respectfully asserts that the subject matter of such claims is deemed novel in view of the arguments made hereinabove.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A system for providing passive screening of transient messages in a distributed computing environment, comprising:
a network interface passively monitoring a transient packet stream at a network boundary comprising receiving incoming datagrams structured in compliance with a network protocol layer;
a packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer;
an antivirus scanner scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents; and
a protocol-specific module processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram.

2. (Original) A system according to Claim 1, further comprising:
an incoming queue staging each incoming datagram intermediate to reassembly.

3. (Original) A system according to Claim 1, further comprising:
a network protocol-specific decoder decoding the reassembled segment prior to scanning.

4. (Original) A system according to Claim 1, wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware.

5. (Original) A system according to Claim 1, wherein the antivirus scanner takes an action if the reassembled segment is infected with at least one of a computer virus and malware.

6. (Original) A system according to Claim 5, wherein the action comprises at least one of logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram; and acquiescing to the infection.

7. (Original) A system according to Claim 1, further comprising:
a protocol-specific queue staging each reassembled segment with other reassembled segments sharing the same transport protocol layer.

8. (Original) A system according to Claim 7, further comprising:
an information record storing information dependent on the same transport protocol layer with the staged reassembled segment.

9. (Original) A system according to Claim 8, further comprising:
a contents record storing the contents with the staged reassembled segment.

10. (Original) A system according to Claim 8, wherein the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject.

11. (Cancelled)

12. (Cancelled)

13. (Original) A system according to Claim 1, further comprising:
an event correlator analyzing the transient packet stream for events indicative of a network service attack.

14. (Original) A system according to Claim 13, further comprising:
a data repository maintaining each event.

15. (Original) A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

16. (Previously Presented) A method for providing passive screening of transient messages in a distributed computing environment, comprising:
passively monitoring a transient packet stream at a network boundary comprising receiving incoming datagrams structured in compliance with a network protocol layer;
reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer;
scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents; and
processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram.

17. (Original) A method according to Claim 16, further comprising:
staging each incoming datagram intermediate to reassembly.

18. (Original) A method according to Claim 16, further comprising:
decoding the reassembled segment prior to scanning.

19. (Original) A method according to Claim 16, further comprising:
terminating the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware.

20. (Original) A method according to Claim 16, further comprising:
taking an action if the reassembled segment is infected with at least one of a computer virus and malware.

21. (Original) A method according to Claim 20, further comprising:
executing the action, comprising at least one of:
logging an infection;
generating a warning;
spoofing a valid datagram in place of the infected datagram; and
acquiescing to the infection.

22. (Original) A method according to Claim 16, further comprising:
staging each reassembled segment with other reassembled segments sharing the same transport protocol layer.

23. (Original) A method according to Claim 22, further comprising:
storing information dependent on the same transport protocol layer with the staged reassembled segment.

24. (Original) A method according to Claim 23, further comprising:
storing the contents with the staged reassembled segment.

25. (Original) A method according to Claim 23, wherein the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject.

26. (Cancelled)

27. (Cancelled)

28. (Original) A method according to Claim 16, further comprising:
analyzing the transient packet stream for events indicative of a network service attack.

29. (Original) A method according to Claim 28, further comprising:
maintaining each event in a data repository.

30. (Original) A method according to Claim 16, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

31. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 28, 29, or 30.

32. (Previously Presented) A system for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising:
a network interface receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied from a packet stream:
a packet receiver reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue;
an antivirus scanner scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware; and
an event correlator evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain;
wherein each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram.

33. (Original) A system according to Claim 32, further comprising:
a parser parsing each reassembled datagram into network protocol-specific information and packet content.

34. (Original) A system according to Claim 33, wherein the network protocol-specific information comprises a source address, source port number, destination address, destination port number, and URL for HTTP; a file name and user name for FTP; and a sender identification, recipient identification, and subject for SMTP.

35. (Original) A system according to Claim 33, further comprising:
a decoder decoding the packet content prior to performing the operation of scanning.

36. (Original) A system according to Claim 32, further comprising:
a log logging an occurrence of at least one of the infection and the network attack.

37. (Original) A system according to Claim 32, further comprising:
a warning module generating a warning responsive to an occurrence of at least one of the infection and the network attack.

38. (Original) A system according to Claim 32, further comprising:
a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack.

39. (Cancelled)

40. (Original) A system according to Claim 32, wherein the distributed computing environment is TCP/IP-compliant, each datagram is IP-compliant, and each network protocol packet is TCP-compliant.

41. (Previously Presented) A method for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising:
receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied from a packet stream;
reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue;
scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware; and
evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain;
wherein each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram.

42. (Original) A method according to Claim 41, further comprising:
parsing each reassembled datagram into network protocol-specific information and packet content.

43. (Original) A method according to Claim 42, wherein the network protocol-specific information comprises a source address, source port number, destination address, destination port number, and URL for HTTP; a file name and user name for FTP; and a sender identification, recipient identification, and subject for SMTP.

44. (Original) A method according to Claim 42, further comprising:
decoding the packet content prior to performing the operation of scanning.

45. (Original) A method according to Claim 41, further comprising:
logging an occurrence of at least one of the infection and the network attack.

46. (Original) A method according to Claim 41, further comprising:
generating a warning responsive to an occurrence of at least one of the infection and the network attack.

47. (Original) A method according to Claim 41, further comprising:
sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack.

48. (Cancelled)

49. (Original) A method according to Claim 41, wherein the distributed computing environment is TCP/IP-compliant, each datagram is IP-compliant, and each network protocol packet is TCP-compliant.

50. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 41, 42, 43, 44, 45, 46, 47, or 49.

51. (Previously Presented) A system according to Claim 32, wherein the network protocol packets employ at least one of HTTP, FTP, SMTP, POP3, NNTP, and Gnutella network protocols.

52. (Previously Presented) A system according to Claim 32, wherein only datagrams compliant with IP protocol are reassembled.

53. (Previously Presented) A system according to Claim 32, wherein the antivirus scanner includes a plurality of protocol-specific scanning submodules, each protocol-specific scanning submodule designated for scanning network protocol packets of a particular protocol.

54. (Previously Presented) A system according to Claim 53, wherein the protocol-specific scanning submodules include an HTTP submodule, an FTP submodule, an SMTP submodule, and an NNTP submodule.

55. (Previously Presented) A system according to Claim 1, wherein the incoming datagrams include IP datagrams that are reassembled into TCP segments.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P393/01.162.01).

Respectfully submitted,

By: _____ Date: 4/3/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660